

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11341268 A**

(43) Date of publication of application: **10 . 12 . 99**

(51) Int. Cl.

**H04N 1/387**  
**H04N 7/24**

(21) Application number: **11089986**

(22) Date of filing: **30 . 03 . 99**

(30) Priority: **30 . 03 . 98 US 98 52041**

(71) Applicant: **SEIKO EPSON CORP**

(72) Inventor: **BHASKARAN VASUDEV**  
**RATNAKAR VIRESH**

(54) **METHOD FOR INSERTING WATERMARK TO DIGITAL IMAGE OR COMPRESSED DIGITAL IMAGE, DIGITAL IMAGE CAPTURING DEVICE, COMPUTER SYSTEM AND METHOD FOR DETECTING ALTERATION OF DIGITAL IMAGE WITH WATERMARK**

(57) Abstract:

PROBLEM TO BE SOLVED: To reduce distortion and to easily verify alteration by partially decoding digital images, generating plural data blocks, judging whether or not to bury watermark bits and burying the watermark bits in the data blocks.

SOLUTION: Images are partially decoded, plural blocks are generated and the quantization variable of the

conversion coefficient of a highest frequency in the respective blocks is obtained and multiplied with the conversion coefficient. Whether or not to bury the watermark bit is judged based on the coefficient and the remaining watermark bit number of the watermark to be buried, the least significant bit of the conversion coefficient of the highest frequency of the block for which burying is decided is set to zero and a hash value calculated in the last block is turned to the hash value of the entire images. Then, by calculating the watermark from the hash value by using a secret key and digital signature algorithm, a ciphered hash value is obtained and the LSB of the conversion coefficient of the block to perform burying is matched with the watermark bit.

COPYRIGHT: (C)1999,JPO

(51) Int.Cl.<sup>5</sup>H 0 4 N 1/387  
7/24

識別記号

F I

H 0 4 N 1/387  
7/13

Z

審査請求 未請求 請求項の数21 O L (全 13 頁)

(21) 出願番号 特願平11-89986

(22) 出願日 平成11年(1999) 3 月30日

(31) 優先権主張番号 0 9 / 0 5 2 , 0 4 1

(32) 優先日 1998年 3 月30日

(33) 優先権主張国 米国 (U S)

(71) 出願人 000002369

セイコーエプソン株式会社

東京都新宿区西新宿 2 丁目 4 番 1 号

(72) 発明者 ヴァスデブ パスカラン

アメリカ合衆国カリフォルニア州94043

マウンテンビュー ノースウィスマンロー  
ド100

(72) 発明者 ヴィレッシュ ラトナカー

アメリカ合衆国カリフォルニア州サニーベ  
イル コルトマデラアベニュー970 アバ  
ートメント402

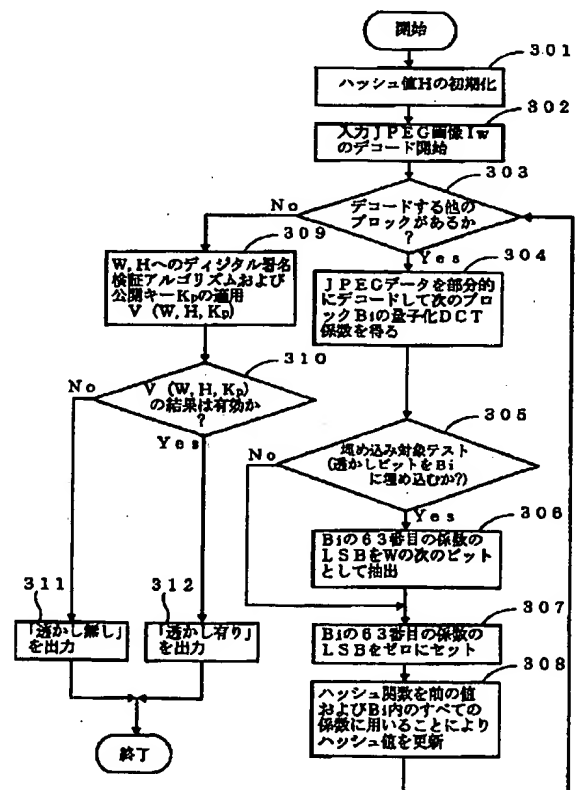
(74) 代理人 弁理士 鈴木 喜三郎 (外 2 名)

(54) 【発明の名称】 デジタル画像または圧縮デジタル画像への透かし挿入方法、デジタル画像キャプチャリング装置、コンピュータシステム、および透かし入りデジタル画像の改ざん検出方法

## (57) 【要約】

【課題】 圧縮デジタル画像の周波数ドメインにおいて脆弱な透かしを直接挿入または抽出する手法およびそのような透かし入りデジタル画像の改ざんの有無を測定する手法を提供する。

【解決手段】 透かしの挿入は、デジタル画像の周波数関数にデジタル画像のハッシュ関数のデジタル署名のビットを埋め込むことで行う。改ざんの検出は、透かし挿入ステップの間に埋め込まれた脆弱透かしをデジタル画像から抽出し、デジタル画像のハッシュ関数を挿入ステップと同様に計算し、公開キーを用いて、抽出した透かしがハッシュ値の有効署名であるか否かを検証することで行う。有効であれば、そのデジタル画像は改ざんされていないことになり、有効でなければ、そのデジタル画像が改ざんされたことになる。



【特許請求の範囲】

【請求項1】 デジタル画像に透かしを挿入する方法において、

圧縮デジタル画像を部分的にデコードして、それぞれが複数の変換係数を有してなる複数のデータブロックを生成するステップ、

前記各データブロックの複数の変換係数の一係数およびデジタル画像に埋め込むべき透かしの残り透かしビット数に基づき、当該データブロックに透かしビットを埋め込むか否かを判断するステップ、

デジタル署名アルゴリズムおよびシークレットキーを用いて、複数のビットを有する透かしをデジタル画像全体について計算するステップ、および、

前記した各データブロックの複数の変換係数の一係数に、前記の計算した透かしの対応するビットをマッチさせるようにセットすることにより、透かしビットを埋め込むか否かを判断する前記ステップにおいて透かしを埋め込むべく判断された各データブロックに、透かしビットを埋め込むステップ、を含むことを特徴とするデジタル画像への透かし挿入方法。

【請求項2】 前記した各データブロックの複数の変換係数の一係数が、当該データブロックの最高周波数を表わす変換係数であることを特徴とする請求項1に記載の圧縮デジタル画像への透かし挿入方法。

【請求項3】 透かしを計算する前記ステップが、透かしビットを埋め込むか否かを判断する前記ステップにおいて透かしを埋め込むべきと判断された各データブロックの、複数の変換係数の一係数の少なくとも1ビットをゼロにセットするステップをさらに含んでなることを特徴とする請求項1または2に記載の圧縮デジタル画像への透かし挿入方法。

【請求項4】 透かしを埋め込む前記ステップが実行された後に、部分的にデコードされた前記複数のデータブロックをエンコードして、透かし入りデジタル画像を再圧縮するステップをさらに含んでなることを特徴とする請求項1～3の何れかに記載の圧縮デジタル画像への透かし挿入方法。

【請求項5】 透かしを計算する前記ステップが、各データブロックについてハッシュ関数を用いることにより各データブロックでハッシュ値を更新するステップをさらに含み、最後のデータブロックについて計算されたハッシュ値がデジタル画像全体を表わす多重ビットのハッシュ値であることを特徴とする請求項1～4の何れかに記載の圧縮デジタル画像への透かし挿入方法。

【請求項6】 透かしを計算する前記ステップが、各データブロックの複数の変換係数の一係数の量子化変数を得るステップ、および各データブロックの変換係数の一係数を前記量子化変数と掛け合わせるステップをさらに含んでなる請求項1～5の何れかに記載の圧縮デジタル画像への透かし挿入方法。

【請求項7】 デジタル画像に透かしを挿入する方法において、

複数のビットを有する透かしをデジタル画像全体について計算するステップを有し、当該ステップが、

圧縮デジタル画像を部分的にデコードして、それぞれが複数の変換係数を有してなる複数のデータブロックを生成するステップ、

各データブロックの複数の変換係数の一係数について量子化変数を得るステップ、

前記の各データブロックの複数の変換係数の一係数を、前記量子化変数と掛け合わせるステップ、

前記各データブロックの最高周波数を表す、当該データブロックの複数の変換係数の一係数およびデジタル画像に埋め込むべき透かしの残り透かしビット数に基づき、各当該データブロックに透かしビットを埋め込むか否かを判断するステップ、

透かしビットを埋め込むか否かを判断する前記ステップにおいて透かしを埋め込むべく判断された各データブロックの複数の変換係数の一係数の少なくとも1ビットをゼロにセットするステップ、

各データブロックについてハッシュ関数を用いることにより各データブロックについてハッシュ値を更新し、最後のデータブロックにおいて計算されたハッシュ値がデジタル画像全体を表わす多重ビットのハッシュ値となるステップ、およびシークレットキーおよびデジタル署名アルゴリズムを多重ビットのハッシュ値に用いて透かしを計算するステップ、を含み、さらに、

当該データブロックの複数の変換係数の一係数の少なくとも1ビットに、前記計算された透かしの対応するビットをマッチさせるようにセットすることにより、透かしビットを埋め込むか否かを判断する前記ステップにおいて透かしを埋め込むべきと判断された各データブロックに、透かしビットを埋め込むステップを有する、ことを特徴とする圧縮デジタル画像への透かし挿入方法。

【請求項8】 透かし入りデジタル画像の改ざんを検出する方法において、

圧縮した透かし入りデジタル画像を部分的にデコードして、それぞれが複数の変換係数を有してなる複数のデータブロックを生成するステップ、

透かしビットが埋め込まれるデータブロックを判断するステップ、

透かしビットが埋め込まれるデータブロックを判断する前記ステップにおいて透かしビットの埋め込み対象であると判断した各データブロックから、当該データブロックの複数の変換係数の一係数から少なくとも1ビットを抽出して抽出透かしを生成するステップ、

最後のデータブロックについて計算されたハッシュ値がデジタル画像全体を表わす多重ビット値であり、当該データブロックの複数の変換係数の一係数の少なくとも1ビットのゼロ化された値に基づいて、各データブロックについてハッシュ関数を用いることにより、デジタル画像のハッシュ値を計算するステップ、および、抽出された透かしおよび多重ビットで計算されたハッシュ値ならびに公開キーに、デジタル署名アルゴリズムを用いて、圧縮デジタル画像が改ざんされたか否かを判断するステップ、

含むことを特徴とする圧縮デジタル画像への透かし挿入方法。

【請求項 9】 各データブロックの複数の変換係数の一係数が、当該データブロックの最高周波数を表わす変換係数である請求項 8 に記載の圧縮デジタル画像への透かし挿入方法。

【請求項 10】 光をキャプチャリングし、その光をアナログデジタル画像信号に変換するセンサと、アナログデジタル画像信号をデジタル画像信号に変換するアナログ-デジタル変換器と、デジタル画像を圧縮して、それぞれが複数の変換係数を有する複数のデータブロックを生成し、当該データブロックの複数の変換係数の一係数およびデジタル画像に埋め込まれるべき透かしの残り透かしビット数に基づいて、各データブロックに透かしビットを埋め込むか否かを判断し、複数のビットを有する透かしのデジタル画像全体について計算し、当該データブロックの複数の変換係数の一係数に、前記の計算した透かしの対応するビットをマッチさせるようにセットすることにより、透かしの埋め込むべく判断された各データブロックに、透かしビットを埋め込むデジタル画像プロセッサと、からなるデジタル画像キャプチャリング装置。

【請求項 11】 前記のデジタル画像プロセッサが、透かしビットを埋め込むべく判断された各データブロックの複数の変換係数の一係数の少なくとも 1 ビットをゼロにセットしてなる請求項 10 に記載のデジタル画像キャプチャリング装置。

【請求項 12】 前記のデジタル画像プロセッサが、透かしビットの埋め込みを完了した後に、透かしが埋め込まれた複数のデータブロックをエンコードして透かし入りデジタル画像を再圧縮してなる請求項 10 または 11 に記載のデジタル画像キャプチャリング装置。

【請求項 13】 前記のデジタル画像プロセッサが、各データブロックについてハッシュ関数を用いることにより各データブロックについてハッシュ値を更新するものであって、最後のデータブロックで計算されたハッシュ値がデジタル画像全体を表わす多重ビットのハッシュ値であることを特徴とする請求項 10 ~ 12 の何れかに記載のデジタル画像キャプチャリング装置。

【請求項 14】 前記のデジタル画像プロセッサが、各データブロックの複数の変換係数の一係数の量子化変数を取得し、当該データブロックの複数の変換係数の一係数を、前記量子化変数と掛け合わせることを特徴とする請求項 10 ~ 13 の何れかに記載のデジタル画像キャプチャリング装置。

【請求項 15】 プロセッサが、圧縮透かし入りデジタル画像の改ざんを検出するように組み込まれたコンピュータ可読プログラムコードを有する、プロセッサおよびメモリを含むコンピュータシステムにおいて、圧縮した透かし入りデジタル画像を部分的にデコードして、各それぞれが複数の変換係数を有してなる複数のデータデータブロックを生成するステップ、

透かしビットが埋め込まれるべきデータブロックを判断するステップ、

透かしビットが埋め込まれるべきデータブロックを判断する前記ステップにおいて透かしビットの埋め込み対象

であると判断された各データブロックから、当該データブロックの複数の変換係数の一係数のうち、少なくとも 1 ビットを抽出して、抽出された透かしを生成するステップ、

最後のデータブロックで計算されたハッシュ値がデジタル画像全体を表わす多重ビット値である、当該データブロックの複数の変換係数の一係数の少なくとも 1 ビットのゼロ化された値に基づいて、各データブロックについてハッシュ関数を用いることにより、デジタル画像のハッシュ値を計算するステップ、および、

デジタル署名アルゴリズムを用いることにより、抽出された透かしと多重ビット値とを比較して、圧縮透かし入りデジタル画像が改ざんされたか否かを判断するステップ、を実行することを特徴とするコンピュータシステム。

【請求項 16】 各データブロックの複数の変換係数の一係数が当該データブロックでの最高周波数を表わす変換係数であることを特徴とする請求項 15 に記載のコンピュータシステム。

【請求項 17】 複数の画素を有するデジタル画像に透かしの挿入する方法において、

複数のビットを有する透かしのデジタル画像全体について計算するステップを有し、当該ステップが、

当該画素を表わす複数のビットの一つおよびデジタル画像に埋め込むべき透かしの残留透かしビット数に基づき、各データブロックに透かしビットを埋め込むか否かを判断するステップ、

透かしビットを埋め込むべく判断する前記の判断ステップで判断される各画素の少なくとも一つのビットをゼロにセットするステップ、

ハッシュ関数を用いることにより各画素でハッシュ値を更新するステップであって、最後の画素で計算されたハッシュ値がデジタル画像全体を表わす多重ビットのハッシュ値であるステップ、および、

シークレットキーおよびデジタル署名アルゴリズムを多重ビットのハッシュ値に用いて透かしの計算するステップを含み、

かつ、

当該画素の少なくとも 1 ビットに、計算された透かしの対応するビットをマッチさせるようにセットすることにより、透かしビットを埋め込むか否かを判断する前記ステップにおいて透かしの埋め込むべく判断された各画素に、透かしビットを埋め込むステップ、を含むことを特徴とするデジタル画像への透かし挿入方法。

【請求項 18】 少なくとも一つのビットは最小有効ビットである請求項 17 に記載のデジタル画像への透かし挿入方法。

【請求項 19】 複数の画素を有する透かし入りデジタル画像の改ざんを検出する方法において、

透かしビットが埋め込まれる各画素を判断するステップ、前記の判断ステップで透かしビットの埋め込み対象であると判断した各画素から、当該画素を表わす複数のビットの少なくとも 1 ビットを抽出して、抽出透かしを生成するステップ、

最後の画素について計算されたハッシュ値がデジタル画像全体を表す多重ビット値であり、当該画素のビットの少なくとも1ビットのゼロ化された値に基づいて、各画素についてハッシュ関数を用いることにより、デジタル画像のハッシュ値を計算するステップ、および、抽出された透かしおよび多重ビットで計算されたハッシュ値ならびに公開キーにデジタル署名検証アルゴリズムを用いて、圧縮デジタル画像が改ざんされたか否かを判断するステップ、を含むことを特徴とする透かし入りデジタル画像の改ざん検出方法。

【請求項20】 少なくとも1ビットは最小有効ビットである請求項19に記載のデジタル画像の改ざん検出方法。

【請求項21】 圧縮デジタル画像に透かしを挿入する方法において、  
目視可能な透かしを加えるステップ、  
デジタル画像および目視可能な透かしから目視不可能な透かしを計算するステップを有し、当該ステップは、圧縮デジタル画像を一部デコードして、各データデータブロックが複数の変換係数を有する複数のデータデータブロックを生成するステップ、  
各データブロックの複数の変換係数の一係数の量子化変数を取得するステップ、  
各データブロックの複数の変換係数の一係数を量子化変数と掛け合わせるステップ、  
当該データブロックの最高周波数を表す、当該データブロックの複数の変換係数の一係数およびデジタル画像デジタル画像に埋め込むべき透かしの残り透かしビット数に基づき、各データブロックに透かしビットを埋め込むか否かを判断するステップ、  
目視可能な透かしビットを埋め込むべく判断する前記ステップにおいて判断される各データブロックの複数の変換係数の一係数の少なくとも1ビットをゼロにセットするステップ、

ハッシュ関数を用いることにより各データブロックでハッシュ値を更新するステップであって、最後のデータブロックで計算されたハッシュ値がデジタル画像全体を表す多重ビットのハッシュ値であるステップ、および、

シークレットキーおよびデジタル署名アルゴリズムを多重ビットのハッシュ値に用いて目視可能な透かしを計算するステップ、を含む、

かつ、

当該データブロックの複数の変換係数の一係数の少なくとも1ビットに、前記計算された目視可能な透かしの対応するビットをマッチさせるようにセットすることにより、データブロックに透かしビットを埋め込むか否かを判断する前記ステップにおいて、透かしを埋め込むべく判断された各データブロックに目視可能な透かしビットを埋め込むステップ、を有することを特徴とする圧縮デジタル画像への透かし挿入方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、一般には脆弱透かし

挿入技術に関し、さらに詳しくは圧縮デジタル画像の周波数ドメインにおいて脆弱な透かしを直接挿入あるいは抽出する技術およびそのような透かし入りデジタル画像の改ざんがなされたか否かを測定する技術に関する。【0002】

【従来の技術】 透かし（ウォーターマーク）とはデジタル画像のようなデジタル創作物に埋め込まれたデジタルパターンである。デジタル画像に透かしを挿入する処理は、圧縮デジタル画像で典型的に用いられる、周波数ドメイン（周波数領域）表現において直接行うことができる。

【0003】 透かしは、歪みの発生を最小限に抑えつつ、ある周波数係数を変更することによって挿入することができる。JPEGデジタル画像圧縮標準で用いられているような、ブロック基準の周波数ドメイン表現の場合、周波数とともにブロックも変更の対象として選ぶことにより歪みを少なくすることができる。いずれの場合も透かしがデジタル画像に挿入された後でその透かしを有効なものとするには、典型的には、ある種のソフトウェアを用いてインプリメントする手順が必要とされる。

【0004】 透かしには異なる種類があり、異なった目的で用いられる。例えば、改ざんに耐える透かしは、デジタル画像の所有者または特定受権者を同定するように設計されている。同定手段として有効に透かしを機能させる（すなわち、デジタル画像の不正な頒布をトレースあるいは追跡する）ためには、デジタル画像を視覚的に傷つけずには透かしを取り除くことが不可能となるか、または少なくとも困難にするようにして、改ざんに耐える透かしをデジタル画像に埋め込まねばならない。また、このような透かしは、デジタル画像処理技術、例えばクロッピング、スケーリング、デジタル画像のエンハンスメント、圧縮／伸張（コンプレス／デコンプレス）等にも耐えるものでなければならない。さらに、改ざんに耐える透かしは、何者かがデジタル画像を改ざんしたとしても、正当な所有者が容易に検出、再生して、デジタル画像の頒布をトレースし、デジタル画像を同定できるようにすべきである。 frag. 6

【0005】 別の種類の透かしは脆弱透かしとも呼ばれ、デジタル画像の改ざんを検出するために設計されている。脆弱透かしは、もし誰かがデジタル画像を改ざんすれば、その改ざんにより透かしが変更または破壊されるように埋め込まれている。脆弱透かしは、例えば、デジタルカメラで生成したデジタル画像との関連では、デジタル画像が作られた後に改ざんしたか否かを判断する基準を設けるのに用いることができる。

【0006】 これまでに多くの透かし挿入法が提案されている。例えば、米国特許第5,530,759号明細書には、線形カラー空間内の原デジタル画像の画素サンプル値に対する多重修正として、その原デジタル画像にデジタル透かしを用いて、画素の色度が変わらないようにすることが提案されている。この手順により、単純に原デジタル画像に加えられた目に見える透かしが得られる。

【0007】 米国特許第5,606,609号明細書には

電子ドキュメント確認システムおよび方法が記載されている。この特許はドキュメントに電子的に署名することを扱っているが、その署名はドキュメントデータ自体に埋め込まれるものではない(すなわち、ドキュメントデータは変更されない)。署名は別のフィールドとしてドキュメントに単に加えられるだけである。

【0008】米国特許第5,613,004号および5,687,236号明細書は、ステガノグラフィ(一目瞭然ではない情報の隠蔽)および暗号法(セキュリティなしの手段で送られる情報のスクランプリング)を統合したものである。データに透かしを入れておき、もしそれがコピーされた場合には、オリジナルの所有者を判定することができる。したがって、これらの特許の透かし挿入方式は改ざんに耐える得る形式である。

【0009】米国特許第5,664,018号明細書では、デジタイズされた画像のコピーの各セットが、わずかに修正された形の「ベースライン」透かしを有する、透かし挿入法が提案されており、「ベースライン」透かしは、データのあるクリティカル領域内に位置する。この方法は改ざんに耐える方式に属するものであって、単一デジタル画像の異なる透かし入りコピーを有する複数の者が共同して透かしを除こうとしても、内容を壊さずに透かしを除きにくくしてある。

【0010】米国特許第5,689,587号明細書には、デジタル画像内のデータを隠蔽する方法および装置について記載されている。この特許はデジタル画像内の情報を隠蔽する方法であって、改ざんへの対抗(著作権型の保護)を保証するものである。

【0011】

【発明が解決しようとする課題】しかし、いずれの特許も改ざんを検出するための脆弱透かし方式を提供するものではない。さらに、いずれの特許も、デジタル画像の周波数ドメイン表現内に直接インプリメントして、埋め込んだ透かしに起因する歪みを最小限に止める透かし挿入技術を提供するものではない。しかも、これらの特許のその他の欠点は、圧縮デジタル画像の完全な伸張を必須とせずには挿入および検証の手順を行ない得ない点である。

【0012】したがって、本発明の目的は上述の問題を克服することである。

【0013】本発明の他の目的は、周波数ドメインにおいて脆弱透かしを挿入および抽出し、また透かしを挿入したデジタル画像が改ざんを受けたか否かを検証するための方式を提供することである。

【0014】本発明のさらに他の目的は、デジタル画像のための脆弱透かし挿入方式との関連で検証の手順を提供することにあり、もし改ざんが発生した場合には、当該検証の手順が、壊された透かしを明らかにし、かつそのデジタル画像の改ざんの発生を知らせる基準を設けるようにすることである。

【0015】本発明のさらに他の目的は、シークレットキーを挿入ステップでのみ使い、他方、検証は公開キーを用いて行う、周波数ドメインでの透かしの挿入および検証法を提供することである。

【0016】本発明のさらに他の目的は、圧縮デジタル

画像の完全伸張を必要としない透かし挿入および検証法を提供することである。

【0017】

【課題を解決するための手段】本発明の一態様によれば、デジタル画像に脆弱透かしを埋め込む技術、およびこのようにして透かしを入れたデジタル画像の改ざんを検出する技術が提供される。

【0018】本発明の別の態様には、圧縮デジタル画像を完全に伸張することなく当該圧縮デジタル画像に透かしを入れ、また、このようにして透かしを入れた圧縮デジタル画像の改ざんを検出することが含まれる。

【0019】本発明のさらに別の態様には、挿入メカニズムではシークレットキーを用い、対応する検証メカニズムでは公開キーを用いるものが含まれる。

【0020】圧縮デジタル画像への透かし挿入には、最初にそのデジタル画像についてハッシュ値を計算することが含まれるが、この計算は次のようにして行われる。すなわち、圧縮デジタル画像を部分的にデコードして、それぞれが複数の変換係数を有する複数のブロックを生成する。各ブロックの中で最高周波数の変換係数についての量子化変数を得て、前記変換係数と前記量子化変数を掛け合わせる。つぎに、各ブロックにおける最高周波数の係数、およびデジタル画像に埋め込まれるべき透かしの残り透かしビット数に基づいて、ブロックに透かしビットを埋め込むか否かを判断する。そして透かしビットを埋め込むと決まったブロックの最高周波数の変換係数の最下位ビット(LSB)をゼロにセットし、各ブロックについてハッシュ関数を用いてハッシュ値を更新する。ここで、最後のブロックで計算したハッシュ値は、デジタル画像全体のハッシュ値を表す多重ビット値である。

【0021】デジタル画像全体についてのハッシュ値が計算されると、シークレットキーおよびデジタル署名アルゴリズムを用いて、計算済みのハッシュ値から透かしが計算される。すなわち、暗号化されたハッシュ値が求められる。

【0022】次いで、先に透かしの埋め込みを行うべきと判断されたブロックにおける最高周波数の変換係数のLSBを、対応する透かしビットにマッチさせるようにセットする。これにより、透かしの埋め込みを行うべきブロックに透かしビットが埋め込まれる。

【0023】そして、透かしを埋め込んだデジタル画像が改ざんされたか否かを判断するために以下のステップが行われる。

【0024】すなわち、透かしを埋め込んだ圧縮デジタル画像を部分的にデコードして、それぞれが複数の変換係数を有する複数のブロックを生成する。

【0025】そして、透かしビットが埋め込まれている各ブロックを判断する。つぎに、透かしビットが埋め込まれたものとして予め判断された各ブロックから、そのデータブロックにおける最高周波数の係数のLSBを抽出して抽出透かしを生成する。LSBがゼロにセットされたデータブロックにおける最高周波数の変換係数の値に基づき、各データブロックでのハッシュ関数を適用することにより、デジタル画像のハッシュ値を計算し(なお、

このデータブロックでは最後のデータブロックで計算したハッシュ値がデジタル画像全体を表わす多重ビット値である)、抽出された透かしおよび計算されたハッシュ値にデジタル署名アルゴリズムを適用し、かつ公開キーを用いて、透かしを入れた圧縮デジタル画像が改ざんされたか否かを判断する。

【0026】透かし挿入の手順はデジタルカメラのようなデジタル画像キャプチャ装置内で直接行うこともできるし、または適当な構成のコンピュータで行うこともできる。また、このようなコンピュータは、透かし入りのデジタル画像を調べて改ざんが加えられたか否かを判断し、もし改ざんが加えられていれば当該画像が存在している場所を決定するのに用いることができる。

【0027】添付の図面とともに以下の説明および特許請求の範囲により、本発明の上述した以外の目的および内容について十分な理解を得ることができる。

【0028】

【発明の実施の形態】デジタル画像周波数ドメインにおいてデジタル画像に透かしを挿入するため、デジタル画像を一旦走査して、そのデジタル画像のkビットのハッシュ値を表わすHを計算する。そして、デジタル署名アルゴリズムSおよびシークレットキーKSを用いてmビットの透かしW=S(H, KS)を計算する。次いで、デジタル画像への透かし挿入手順の二次パスを用いて、デジタル画像に透かしWが埋め込まれる。これらのステップを図1、図2、図3に示す。

【0029】先ず図2を参照し、次いで図1および図3を参照すると、ステップ101では初期の走査手順でハッシュ値Hが固定値に初期化される。ステップ102では、JPEG画像Iの形態の圧縮デジタル画像がデコーダに送られる。デコーダは、JPEGデータからヘッダを分析し、最高周波数の係数についての量子化テーブルエントリであるqの値を知ることができる。この最高周波数の係数は、JPEGで用いられる8×8離散コサイン変換(DCT)についての63番目の係数である。

【0030】もし、さらにデコードおよび処理(ステップ103)されるべき他のデータブロック(次のデータブロック)があれば、当該次のデータブロックBiはステップ104で部分的にデコードされる。圧縮データのエン트로ピー符号化は行われずに、完全伸張に必要とされるデ・ジグザグ(de-zig-zagging)化、非量子化(dequantization)および逆離散コサイン変換(IDCT)のステップが回避される。そして、ジグザグ順に配置した非ゼロ量子化係数のみからなるデータブロックBiの表現が得られる。

【0031】本発明では、63番目の変換係数を特別に透かし挿入に用いているので、その値がゼロであってもデータブロックBiの表現は常に63番目の変換係数を有する構成となる。すなわち、データブロックBiの表現には常に63番目の係数が情報として含まれる。このようにして、他の非ゼロ量子化係数も、デ・ジグザグ化なしに容易に行うことができることに注意すべきである。なぜなら、63番目の変換係数がジグザグ順の最後の係数であるからである。

【0032】次いでデータブロックBiのデコードされた表現は、ステップ105に渡され、その63番目の変換係数と量子化変数q(ステップ102で得られる)とが掛け合わされる。

【0033】このステップが行われる理由は以下の通りである。より高い周波数における小さな変動は肉眼では判断できない。歪みを最小限に止めるため、透かしWは最高周波数の係数(この場合63番目の係数)のみを変更することによってビット単位で埋め込まれる。

【0034】透かしビットに等しい値に、前記の63番目の変換係数のLSBを変えることにより、透かしビットが係数値に埋め込まれる(後述の図3のステップ207)。63番目の係数の値がvであれば、このLSBの変動により、プラスまたはマイナスq(ここでqは63番目の変換係数の量子化変数である)で非量子化された係数が変動する。この変動を最小にするため、本実施例では63番目の変換係数の量子化変数qを1にセットし、各データブロックにおける63番目の変換係数(埋め込み中の透かしビットではない)を非量子化値(qとの掛け合わせで得られる)と直接置き換える。

【0035】このステップにより、伸張の際の歪みは、プラスまたはマイナス1のみである。63番目の変換係数はほとんどのデータブロックで典型的には、もともとゼロであり、非ゼロ係数のみが圧縮サイズの大半についてあるので、ステップ105での掛け合わせによって生じる圧縮サイズの増加は最小限となる。

【0036】ステップ106では透かしビットをデータブロックBiに埋め込むべきか否かの決定がなされる。ステップ106での決定の手順は、デジタル画像に生じる歪みを最小にするとともに、圧縮デジタル画像のサイズ増も最小にするように設計される。この決定手順は後述の二箇所再度用いられるので、単に埋め込み対象テスト(EMBEDDER-TEST)と呼ぶ。以下、埋め込み対象テストについて詳述する。

【0037】カラーデジタル画像については、透かしはデジタル画像の輝度面にのみ埋め込まれる。この埋め込みは、伸張される間に輝度-色度カラー表示が赤、緑および青の画素値(RGB)に変換されるとき、発生する歪みを最小にするように行われる。さらに、色度面は典型的には準サンプル化されており、したがって単一の色度データブロックにおけるいかなる歪みも数個のRGBデータブロックに歪みを生じる。このため、グレースケールデジタル画像およびカラーデジタル画像では、透かしビットはゼロ付番されたカラー成分(カラーデジタル画像用の輝度面)のみに埋め込まれる。

【0038】前述の通り、歪みを最小にするために透かしビットは63番目のDCT係数にのみ埋め込まれる。圧縮サイズを最小にするために、63番目のDCT係数がすでに非ゼロであるデータブロックのみを選んで、透かしビットを埋め込む。このことは、ゼロ値から非ゼロ値への変化が、非ゼロ値から他のゼロ値への変化に比して、はるかに大きな圧縮サイズをもたらす観察結果に従うものである。

【0039】埋め込み対象テストは透かし検証手順によ



でも行われる。しかし、63番目の係数(非量子化)がプラス1またはマイナス1であるデータブロックでも埋め込み対象としては選ばない。何故なら、透かしビットを埋め込む際にゼロに戻り、そのため検証部が、埋め込まれたデータブロックを決定できなくなるためである。

【0040】埋め込み用に残っている透かしビットの数が、ある時点で、残りのデータブロック数に等しくなれば、残りの各データブロックは透かしビットの埋め込み対象として決定される。

【0041】データブロックBiに透かしビットを埋め込む決定が「YES」であれば、63番目のDCT係数のLSBは、ステップ107でゼロにセットされて、その手順がステップ108に進む。決定が「NO」であれば、この手順は直接ステップ108に進む。ハッシュ値Hはその前の値を用いてステップ108で更新され、そしてジグザグ順に配置した、データブロックBiにおけるすべての非ゼロ量子化係数値は、一方向ハッシュ関数を用いることにより更新される。63番目の係数はゼロであっても常にこのハッシュ値の計算に含まれる。

【0042】すべてのデータブロックが処理されると、手順はステップ109に進み、計算されたハッシュ値HおよびシークレットキーKSにデジタル署名アルゴリズムSが適用されてmビットの透かし $W = S(H, KS)$ を計算する。

【0043】まず、図3を参照し、次いで図1および2を参照すると、透かし挿入手順の二次パスでは、入力JPEGデジタル画像Iが再びデコードに送られるが、デコードは、ステップ201で63番目のDCT係数についての量子化変数であるq値を符号化するヘッダを分析する。

【0044】ステップ202では、透かし入り出力JPEGデジタル画像についてのヘッダIWが入力デジタル画像からの直接コピーによって生成される。ただし、量子化テーブルにおける63番目のDCT係数の量子化変数は、その前の値qの代わりに1に変えられる。さらにデコードされ、処理(ステップ203)されるべき他のデータブロックがあれば、その次のデータブロックBiはステップ204で部分的にデコードされる。前述したと同様に、圧縮画像データのエントロピー符号化は行われず、完全伸張に必要なデ・ジグザグ化、非量子化およびIDCTのステップが回避される。その結果、非ゼロ量子化係数のみからなるBiの表現(ただし、常に当該表現に含まれる63番目の係数については除く)がジグザグ順の配置を伴って生じる。

【0045】ステップ205では、各データブロックの63番目のDCT係数と量子化変数qとが掛け合わされる。埋め込み対象テストがステップ206で行われ、データブロックBiにWの次のビットを埋め込むか否かを判断する。この判断はデータブロック毎に再び行ってもよく、これらの結果がメモリに記憶されれば、前の決定を下すステップ(ステップ105)を用いて行ってもよい。いずれの場合も、データブロックBiにWの次のビットを埋め込むことになれば、ステップ207においてBiの63番目のDCT係数のLSBはWの次のビットにマッチ

するようにセットされ、そして手順は次のステップ208に進む。ステップ206の決定が「NO」であれば、手順は直接ステップ208に進む。

【0046】ステップ208では、データブロックBiにおけるDCT係数がエンコードされ、透かし入りデジタル画像Iwについての圧縮データストリームへの出力として生成される。量子化係数はすでにジグザグ順になっているので、ここで用いるデータブロックBiの量子化係数の表現により、有効なエンコードが可能となり、そのため一般に圧縮に必要なDCT、量子化およびジグザグ化のステップが回避される。このステップはすべてのデータブロックが処理されるまで繰り返される。

【0047】周波数ドメイン透かし挿入法の検証手順を図4および図5に示す。この手順はデジタル画像が改ざんされたか否かを判断するために用いられる。

【0048】図5では、ステップ301でハッシュ値Hが初期化された後、ステップ302では透かし検証手順が起動して入力デジタル画像Iwをデコードし、ヘッダを分析する。ステップ303では、デコードすべきデータブロックが他に残っているか否かを判断する。もし残っていれば、ステップ304で次のデータブロックBiが部分的にデコードされる。ここで再び、圧縮データのエントロピー符号化は行われず、完全伸張に必要なデ・ジグザグ化、非量子化およびIDCTのステップが回避される。この結果、非ゼロ量子化係数のみからなるデータブロックBiの表現(ただし、常に当該表現に含まれる63番目のDCT係数については除く)がジグザグ順の配置を伴って生じる。埋め込み対象テストはステップ305で行われ、データブロックBiに透かしWの次のビットを埋め込むか否かを判断する。

【0049】透かしWを埋め込むべきと判断されると、ステップ306においてデータブロックBiの63番目のLSBは透かしWの次のビットとして抽出され、ステップ307でそのLSBがゼロにセットされる。データブロックBiが透かしビットの埋め込み対象でないときは、手順はステップ307およびステップ305からステップ308に移行する。ハッシュ値Hはその前の値を用いることによりステップ308で更新され、またデータブロックBiにおける非ゼロ量子化係数のすべての値は、ジグザグ順の配置とともに、一方向ハッシュ関数を用いることにより更新される。63番目のDCT係数はゼロであっても常にこのハッシュ値の計算に含まれる。このステップはすべてのブロックを通して継続し、そして最後に抽出された透かしWおよびハッシュ値Hが完全に計算される。

【0050】この時点で、公開キーKp(シークレットキーKSに対応)を用いて、デジタル署名アルゴリズムV(署名アルゴリズムSに対応)に適用され、ステップ309で透かしWが $S(H, KS)$ と同じか否かを検証する。ステップ309はシークレットキーKSの使用を必要としない点に注意すべきである。ステップ310では、ステップ309で適用されたデジタル署名検証アルゴリズムV(W, H, Kp)の出力が調べられる。もし、アルゴリズムV(W, H, Kp)が合格であれば、デジタル



画像は完全な脆弱透かしを有しており、したがって改ざんされていないことになる(ステップ312)。もし、アルゴリズムV(W, H, Kp)が不合格であれば、脆弱透かしは(まだ存在しているとして)すでに破壊されており、したがってデジタル画像は改ざんされたか、キーの対(KS, Kp)に対応する脆弱透かしを有していなかったと結論できる(ステップ311)。

【0051】デジタル画像改ざん検証ステップの効果はハッシュ関数の強さと署名および検証アルゴリズムSおよびVに左右される。種々の一方方向ハッシュ関数を用いることができるが、例えば、アール・リベスト(R. Rivest)が開発したMD5と呼ばれるハッシュ関数、あるいはSHAまたはRIPEMDハッシュ関数がある。同様に、署名および検証アルゴリズムに用い得るものも数多くあり、例えばエルガマル(El Gamal)スキーム、DSAアルゴリズムまたはRSAアルゴリズムがある。

【0052】この脆弱透かし挿入手順を変更して、改ざんがすでになされたデジタル画像の領域を大まかに調べることができる。この方法は、デジタル画像を数個の領域に区分し、各領域に別々にすべての挿入手順を施すことによって行なわれる。改ざんされた箇所を含む領域のみが透かしの破壊を示す。しかし、この変更された手順では制限された形式の改ざんは検出されない。なお、このような改ざんは、異なるデジタル画像から抽出した数領域のカラーズまたは単一デジタル画像からの再配列領域(各領域は有効な透かしをもたらしている)のカラーズであるデジタル画像を形成させることによって行われるものである。しかし、このような改ざんはその領域が十分大きければ一目瞭然である。

【0053】同様な脆弱透かし挿入法は空間領域にも応用することができる。最高周波数の係数の代わりに、すべての画素またはその一部を透かしビット埋め込み対象として直接用い、ハッシュ関数の計算に先だってLSBをゼロにセットし、次いでこのLSBを二次パスにおける透かしビットにセットすることによって行う。本発明は空間および周波数ドメインの透かし挿入法の統合に限定されるものではない。また、本発明は、上述したような透かしの挿入を周波数ドメイン内で行い得るようにし、一方、対応する透かしの検証を上述の通り空間領域内で行うことに限定されるものではない。

【0054】さらに、この透かしは目視可能な透かしとすることができる。特有の透かし信号の変換周波数係数を計算し、これをデジタル画像の係数に単純に追加することにより、目視可能な透かしを周波数ドメインに埋め込むことができる。このステップはデジタル画像のコード化(例えばDCT)で共通に用いられる変換の直線性の結果としての作用をするが、画素領域内でのこのような追加が周波数ドメインでの追加に対応することを保証するものである。同様な目視可能な透かし挿入法は空間領域でも行うことができる。

【0055】本発明の透かし挿入、抽出および検証手順を説明するブロック図および流れ図は、ある特定の機能の実行および関連性を説明するものである点に注意すべき

である。これらの機能的ブロックの境界は説明の都合で任意に限定したものである。特定の機能および関連性が適当に得られる限りにおいて、この境界に代わるものを定めることができる。さらに、この流れ図は、シンタックスまたはいかなる特定のプログラム言語を表わすものではない。むしろこれらの図は、当業者が必要な処理を行うための回路を組み立て、またはソフトウェアを作成するのに必要な機能上の情報を示すものである。ブロック図および流れ図に示す各機能は、例えば、ソフトウェアの命令、デジタル信号処理回路のような機能的に等しい回路、アプリケーションスペシフィック集積回路(ASIC)またはこれらの組合せによってインプリメントされる。

【0056】本発明の透かし挿入法は、そのブロック図を図6に示すデジタルカメラを含む各種装置との関連で用いることができる。デジタルカメラ20は、マイクロプロセッサ制御部でのオペレーションでは、デジタル画像をキャプチャリングし、ブロック21内でアナログ電気信号に変換する電荷結合素子(CCD)からなる画像センサを有する。次いでアナログ信号は処理ブロック22(アナログ信号処理、A/D変換を行う)で処理され、デジタル化され、その後、デジタル画像はフレームバッファ23に一時的に記憶され、同時に処理ブロック24(デジタル画像変換処理を行う)でのデジタル処理に付される。

【0057】処理ブロック24はハードウェアまたはソフトウェアを用いて本発明の透かし挿入を行うが、フレームバッファ23から入力される画像データは圧縮前のデータであるので、該データに対して伸張処理を行うことなくDCT変換し、透かし埋め込みを行う。処理ブロック24は透かし埋め込み後の画像データをJPEG等に圧縮し、ユーザ制御部のもとに、カメラ内蔵の画像記憶装置26に記憶する。記憶ブロック(画像記憶装置26)は、カメラ20と取り外し可能型または固定型のいずれかのコンパクト磁気媒体または固体記憶媒体を有することができるし、また取り外し可能型の大容量PCMCIA仕様のハードディスクカードまたはフラッシュ記憶カードを含むことができる。

【0058】カメラ20は、それぞれアナログ出力部(D/A変換およびアナログ出力を行う)27およびデジタル出力部28を含み、これらを通して画像データがカメラ内または外部装置に転送される。圧縮されない画像データはアナログ出力部27を経由してカメラ20内のLCDスクリーン29に転送されるか、またはVCRやテレビ受像器のような外部装置に転送される。画像データは、圧縮であれ未圧縮であれ、デジタル出力部29を通してコンピュータシステムのようなデジタル装置にも転送され、ここで画像を表示したり、または透かし入り画像を検証することができる。

【0059】図7は、デジタル画像をキャプチャリング、処理、検証するために用いる各種コンポーネント間の相互関係を示すブロック図である。重要なコンポーネントの一つとしてコンピュータシステムがあり、図中では一般に符号30で示す。コンピュータシステム30は、メイ

ンフレームまたはパーソナルコンピュータのような適当な形式のものであってよい。

【0060】コンピュータシステム30は、慣用のマイクロプロセッサである中央処理装置(CPU)31、情報を一時的に記憶するランダムアクセスメモリ(RAM)32および情報を永久に記憶するリードオンリーメモリ(ROM)33からなる。これらの各コンポーネントはバス34と接続している。コンピュータシステム30のオペレーションは、典型的にはオペレーティングシステムのソフトウェアによって制御、調整される。システムメモリに組み込まれ、CPU31上で動作するオペレーティングシステムは、システム資源の配分を制御し、特に処理、メモリ管理、ネットワークングおよびI/O機能のような種々のタスクを行うことによって、コンピュータシステム30のオペレーションを行う。

【0061】また、ディスクett37のような不揮発性大容量記憶装置を挿入するディスクettドライブ36はコントローラ35によりバス34と接続する。同様に、コントローラ38は、バス34とコンパクトディスク(CD)ROM40を受け入れるCDROMドライブ39との間のインターフェースをとる。ハードディスク41は、ディスクettコントローラ43によりバス34と接続する固定ディスクドライブ42の一部として設けられている。

【0062】透かし挿入法のためのソフトウェアは、たとえばハードディスク41に記憶され、実行に際してCPU31に転送される。これとは別に、ソフトウェアをRAM32またはROM33に記憶させてもよい。同様に、ディスクett37およびCDROM40のような取り外し可能な記憶媒体装置を用いて、コンピュータシステム30にデジタル画像データをロードしたり、またはシステムから抽出してもよい。

【0063】デジタル画像データはコンピュータシステム30に入力されるが、別の方法であってもよい。フィルムカメラ45で生成したフィルムベースの画像44は記憶用のスキャナ46によりデジタル化され、コンピュータ30により処理される。デジタルカメラ20は上述の通り画像を直接デジタル化し、これらをコンピュータ30に転送することが可能である。コントローラ53を経由してバス34に接続するキーボード51およびマウス52はこのようなデータの入力を容易にするが、さもないと情報をコンピュータシステム30に入力するための手段を用意することになる。

【0064】また、遠隔配置を目的として、デジタル画像データの転送をコンピュータ30との間で行ってもよい。そのためには、コンピュータ30は通信アダプタ54を含むことができ、このアダプタにより直接接続またはモデム経由のローカルエリアネットワーク(LAN)、インターネットまたはオンラインサービスを含むネットワーク55との通信が可能になる。

【0065】本発明によれば、例えばデジタルカメラ20内で予め透かし入れしたデジタル画像を検証のためにコンピュータ30に転送することができる。これとは別に、透かし無しのデジタル画像に透かしを入れ、そしてCPU31で実行される適当なハードウェアまたはソ

フトウェアを用いて透かし入りデジタル画像をコンピュータ内で検証してもよい。

【0066】コンピュータ30内に転送または蓄積されたデジタル画像は多くの異なる方法で検証することができる。コンピュータ30に付属するプリンタ56はカラー印刷を行うが、その品質はプリンタ56に依存して変動する。その他のオプションとして、コンピュータ30に付属するディスプレイ57上でのデジタル画像の検証がある。さらに別の手段としては、VCRを用いてテレビモニター上にデジタル画像を表示する方法もある。

【0067】以上、特定の具体例により本発明を説明したが、当業者には明らかなように、さらに種々変更を加えることが可能である。例えば、本発明記載の目視可能な透かし挿入法は目視不能な透かし挿入法は、用途によっては組合せることができる。透かし挿入ステップで用いるブロックは用途次第で選択することができる。このように、本発明には特許請求の範囲の精神と範囲内に含まれるすべての変更が包含される。

【0068】

【発明の効果】(1)改ざんを検出するための脆弱透かし方式を提供することができる。

【0069】(2)デジタル画像の周波数ドメインに直接インプリメントすることができるので、埋め込んだ透かしに起因する歪みを最小限に止める透かし挿入技術を提供することができる。

【0070】(3)圧縮デジタル画像の完全伸張を必須とせずに、挿入および検証の手順を行うことができる。

【0071】(4)透かしを挿入したデジタル画像が改ざんを受けたか否かを検証することができる。デジタル画像のための脆弱透かし挿入方式との関連で検証の手順を提供することができ、改ざんが発生したら、検証の手順が壊された透かしを明らかにでき、またそのデジタル画像の改ざん発生を知らせる基準を設けることもできる。

【0072】(5)シークレットキーを挿入ステップでのみ使い、他方、検証は公開キーを用いて行う、周波数ドメイン透かしの挿入および検証を行うことができる。

【図面の簡単な説明】

【図1】本発明によるデジタル画像の周波数ドメインへの透かし挿入を示す一般的な概念図である。

【図2】本発明によるデジタル画像の周波数ドメインへの透かし挿入法に関連して初期の走査手順を示す流れ図である。

【図3】本発明によるデジタル画像の周波数ドメインへの透かし挿入法に関連してデジタル画像にビットを埋め込む手順を示す流れ図である。

【図4】本発明による、周波数ドメインにおける脆弱透かしの存在を透かしデジタル画像から検証することを示す概念図である。

【図5】デジタル画像から透かしを抽出し、透かしの有効性を検証してデジタル画像が改ざんされたか否かを判断する方法を示す流れ図である。

【図6】本発明との関連で用いるために取り付けけたデジタルカメラのブロック図である。

【図7】本発明によるデジタル画像のキャプチャリング

および検証、ならびにこのようなデジタル画像の処理に用いられる種々の成分間の相互関係を示すブロック図である。

【符号の説明】

- 20 デジタルカメラ
- 21 CCDデジタル画像センサ
- 22 アナログ信号処理ブロック
- 23 フレームバッファ
- 24 デジタル画像処理ブロック
- 25 制御部
- 26 インカメラデジタル画像記憶装置
- 27 アナログ出力部
- 28 デジタル出力部
- 29 LCDスクリーン
- 30 コンピュータシステム
- 31 CPU
- 32 RAM
- 33 ROM
- 34 バス
- 35 コントローラ
- 36 ディスケットドライブ
- 37 ディスケット
- 38 コントローラ
- 39 CDROMドライブ
- 40 コンパクトディスク
- 41 ハードディスク
- 42 固定ディスクドライブ
- 43 ディスクコントローラ
- 44 フィルム
- 45 フィルムカメラ
- 46 スキャナ
- 51 キーボード
- 52 マウス
- 53 コントローラ
- 54 通信アダプタ
- 55 ネットワーク
- 56 プリンタ
- 57 ディスプレイ

【図1】

【図2】

【図3】

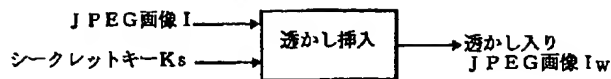
【図4】

【図5】

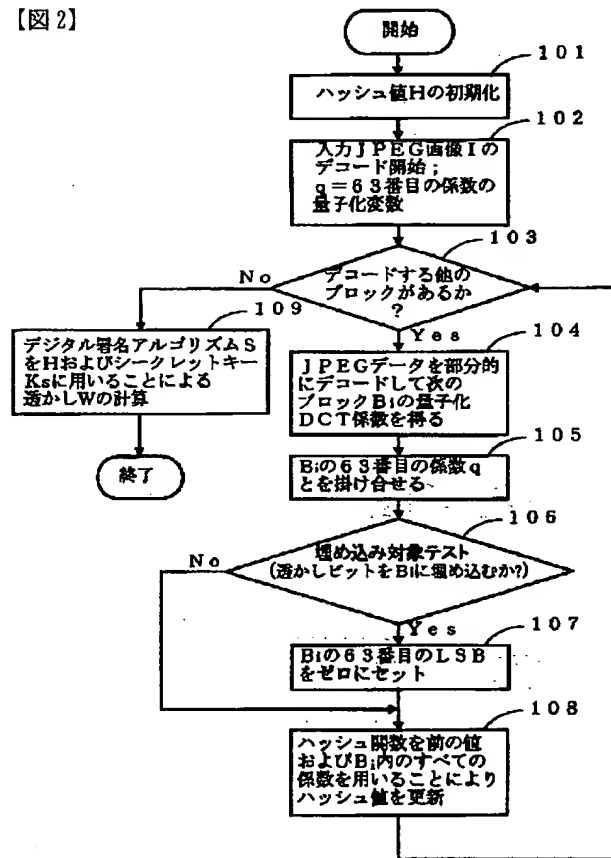
【図6】

【図7】

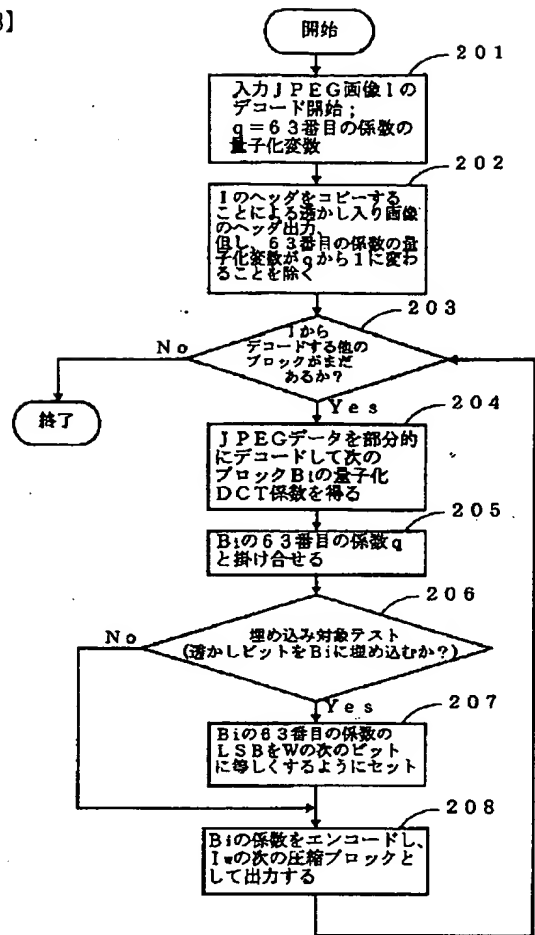
【図1】



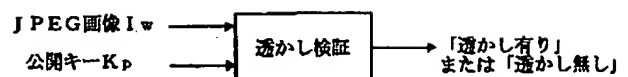
【図2】



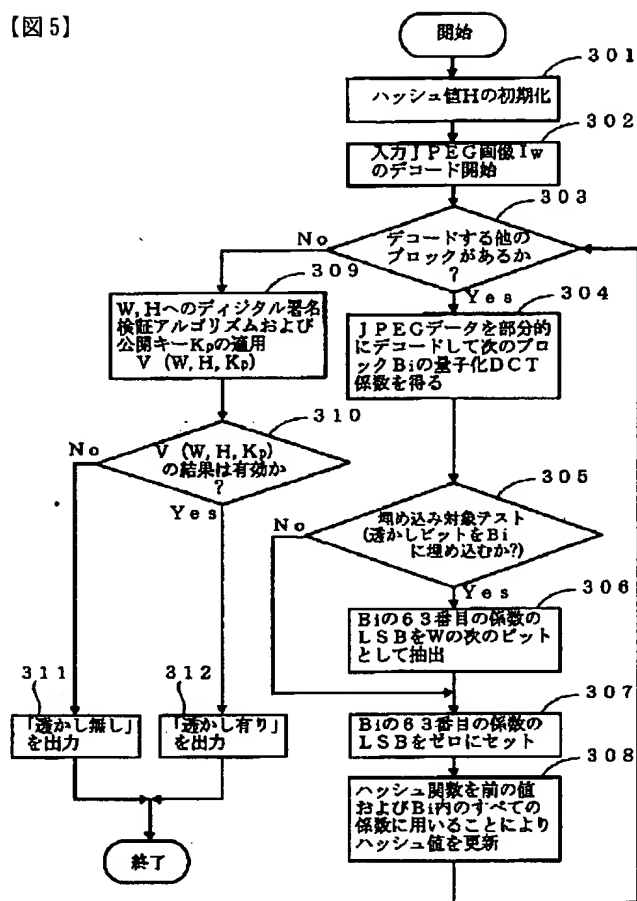
【図3】



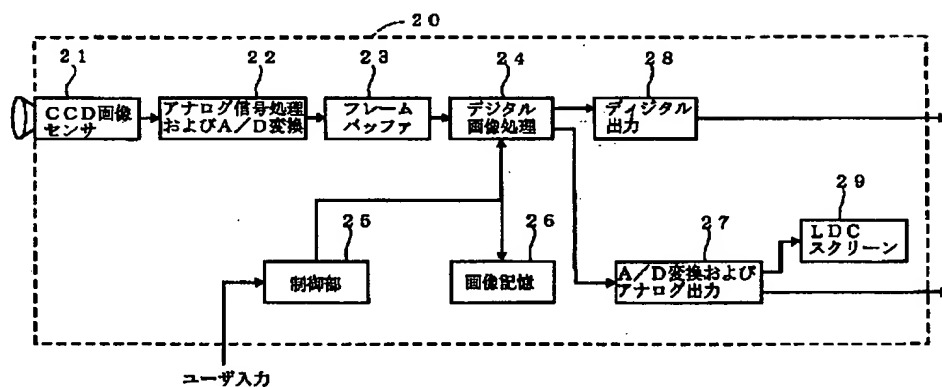
【図4】



【図5】



【図6】



【図7】

